PROCEDURE 1410.24
Issued: March 29, 2001
Effective Date: April 16, 2001

SUBJECT:	Internal Gateway to Internal Gateway Virtual Private Network (VPN)
APPLICATION:	Executive Branch Departments and sub-units and non-executive branch entities when using the State of Michigan (SOM) WAN or LMAN data communication networks for secured encrypted internal host to internal host communication within the Internet Protocol suite (TCP/IP).
PURPOSE:	To standardize an internal gateway to internal gateway VPN security policy and guideline for State of Michigan agencies connecting to internal data communications networks from other internal locations over host networks that are controlled, operated, or managed by or for the State of Michigan.
CONTACT AGENCY:	Department of Information Technology (DIT) Office of Strategic Policy
TELEPHONE:	517/373-7326
FAX:	517/335-2355

SUMMARY:

This procedure establishes **IPSec** used in transport mode as the internal gateway peer to gateway peer technology adhered to in compliance with the State of Michigan security policy as framed by standard 1410.23 and best practice to protect internal networks, devices, and hosts from risk of unauthorized monitoring. The threat posed from transmitting data requiring protection by law or regulation over the internal network does not require, nor will this standard allow encryption of the original source and destination IP addresses.

The **IPSec** structure provides origin authentication, integrity, confidentiality through encryption, and anti-replay security services.

The inclusive transport mechanisms and international standard protocols include:

TCP/IPv4 v6, IPSec, ESP, AH, DES, MD5

Applicable Internet Engineering Task Force (IETF) Request-for-Comments (RFC) includes all current RFCs related to the technology elements and modules previously listed.

APPLICABLE FORMS: None.

PROCEDURES:

General Information:

The objectives of the ***internal gateway to gateway VPN standard*** are to:

Protect State of Michigan internal systems data from unauthorized monitoring or tampering.

Support the secure internal data transfer needs of the State's agencies when required by law or regulation to protect the privacy of citizen information.

Prevent disclosure of information classified as protected under state statute to unauthorized individuals.

Benefits expected:

Increased security for data classified as requiring protection.

Maintain acceptable levels of network management efficiency.

Easier maintenance and enforcement of enterprise level security policies.

Opportunity to integrate Quality of Service (QOS) practices.

Applicability:

Conditions of Application:

This standard applies to non-browser client connections from desktops, laptops, or workstations, servers or hosts that require access to any internal State of Michigan host system, server, or network connected host device. It specifically is applicable when the network, host, or device contains information that is classified as protected under Michigan compiled laws, and the connection is carried over networks that **are** managed by or specifically for the State of Michigan.

All routes redirected for the hosts or client users while attached as traversing the State of Michigan's internal gateway VPN node concentrators will be routed and limited to internal hosts on the LMAN or SOM-WAN exclusively. This standard differs from other VPN standards and applies when both the near-end node and the distant-end node are inside of the SOM trusted network perimeter.

This standard applies to intranet access. Intranet is defined as connections to internal agency LANs, enterprise LMAN, or SOM-WAN where both or all connecting nodes or clients are inside of the State of Michigan trusted network perimeter and the internal destination hosts are on any of the State of Michigan's internal host networks.

This standard does not cover:

1. Host connections where one or more nodes are external to the State of Michigan trusted perimeter networks (LMAN or SOM-WAN).

2. Secure Sockets Layer (SSL) enabled client Web browser applications available to the Internet or Intranets.

3. Intermittent connections made over the public switched telephone network using a plain old telephone (POTS) or integrated services digital network (ISDN) dial-in-connections to the State of Michigan's central modem bank.

4. This standard does not address the total security access needs and is intended to supplement and/or be combined with other security standards and best practices when indicated as necessary to provide adequate risk reduction.

Assumptions:

- Agency hosts are accessing State of Michigan network and server resources with agency provided equipment configured, managed, and maintained by agency technical staff.

- Host applications utilize application layer security best practices such as user name and password, and/or pin number combinations at a minimum, to reduce risk of unauthorized access leading to injurious use.

In addition to use of VPN technology, agency network or host administrators shall provide appropriate security though best practices applicable to application level, network access, or host operating system security.

Implementation considerations:

This standard applies when the internal connections are for same agency to same agency or when different agencies are cooperating on formal internal data sharing agreements.

Agencies must inform the Network Operations Center (NOC) when internal VPNs are planned and review the security risk threat profile analysis with the Enterprise Security Director.

Agencies may deploy their own VPN concentrators, use host systems, or downstream routers managed by the agency to provide **IPsec** enabled VPN tunnels across the intra-net connection points to State of Michigan networks.   The concentrator device should use hardware-based encryption where possible to keep system latency at a minimum level. Issuance of keys for the DES (DES encryption) will require maintaining appropriate logs and documents pertaining to issuance of keys.

Agencies shall establish internal procedures to immediately notify NOC when VPN tunnels should be withdrawn from access control and security association lists maintained by NOC.

Agencies may not, under any circumstances, establish any VPNs tunneled across public networks that are not terminated on DMB concentrators and managed by NOC. Management and operation of all VPNs security associations with a node external to the trusted network perimeter must be handled by the NOC and approved by the Enterprise Security Director.

Technical Considerations: Implementations of multi-node internal VPNs will standardize on pairs of IPSec-enabled peers (gateways or hosts) with security associations configured for using a transport mode only security association with both Encapsulating Security Payload (ESP) and Authentication Header (AH) support and pre-shared or dynamically assigned keys to provide DES (56 bit) encryption. Along with DES encryption use of the MD5 hashing algorithm is mandatory to provide en-route data integrity. Tunnel mode on internal networks (SOM-WAN, L-MAN) is specifically disallowed by this standard. All internal VPNs will be authorized by the agency security administrator and approved by the Enterprise Security Director and registered with the Network Operation Center by a signed letter.

Additional data encapsulation through the use of lower security (under 128 bit) encryption algorithms on the host device or client before passing the data packets to the gateway, where desirable and technically possible, to provide added host application security is not disallowed by this standard. Tunneling of non-IP protocol packets within secure IPSec-IP-packets is allowed by this standard, but must be done by the agency hosts or appliances, and not on the enterprise routers.

Maintenance:

DMB: Acquisition Services shall not approve any acquisition or purchase request without confirmation from the Department of Information Technology, Office of Strategic Policy that such request is in compliance with the standard.

Operational Units: Operating Units (OU) will coordinate internal and external VPN requirements with the NOC and the Enterprise Security Director. Requests to establish VPNs must be signed by the agency security administrator and sent to NOC.

Any and all projects, consulting requests, equipment and software acquisition requests, or ITB's relating to internal gateway to internal gateway VPNs will be subject to review for compliance with this standard.

DIT: The Office of Strategic Policy will review this standard on a continuing basis and make recommendations for changes. An appropriate group of staff, representing a wide-range of state operational units, will review and possibly revise these standards and guidelines as often as needed.

Exceptions from this standard for reasons other than those outlined above will be made through the exception handling process described in the Exception Process Template.

***